Science Journal of Kanagawa University **29** ：33-38 (2018)

■原　著■　2017 年度神奈川大学総合理学研究所共同研究助成論文

形式アシュランスケースのモジュール化事例 ー SDBS の帰属および帰属決定プロセスについての アシュランスケースの研究 ー

渡邊　宏[1,4]　木下佳樹[2,3]　武山　誠[2,3]

A Case Study of Modular Design for Formal Assurance Case

Hiroshi Watanabe[1,4], Yoshiki Kinoshita[2,3] and Makoto Takeyama[2,3]

[1] Research Institute for Materials and Chemical Measurement, National Institute of Advanced Industrial Science and Technology, Tsukuba City, Ibaraki 305-8565, Japan.
[2] Department of Information Science, Faculty of Science, Kanagawa University, Hiratsuka City, Kanagawa 259-1293, Japan.
[3] Research Institute for Programming Science, Kanagawa University, Hiratsuka City, Kanagawa 259-1293, Japan.
[4] To whom correspondence should be addressed. E-mail: hiroshi-watanabe@aist.go.jp

Abstract: We present a case study of modular design for formal assurance case in Agda. The formal assurance case to be decomposed in our study claims the quality and reliability of data, and it was developed in previous work. In this study, we present the following: some requirements for modularization which is obtained from the analysis of both the code and domain of our case; decomposition criteria obtained from the analysis of the requirements. Moreover we give a concrete example of module decomposition of the case based on the criteria.
Keywords: formal assurance case, modular design, Agda, decomposition criteria

序論

モジュール化は、ソフトウェア工学における基本的な設計概念で、システム全体を管理しやすいサイズの小さな部品に分解して構成しようとするものである[1,2]。複雑化、大規模化するシステムを複数人で効率良く開発するため、システムの全体的な理解を促進するため、また、再利用性を高めるために用いられる。

アシュランスケースは安全性、セキュリティ、総合信頼性などについての、システムのアシュランス（システムへの信頼）の議論を明文化したものである。さらにこれを計算機で処理しやすいように形式言語で表現したものは形式アシュランスケースと呼ばれる。特にプログラムの形で形式アシュランスケースを記すことができることが知られている[3]。モジュール化は、プログラムを対象として議論されることから始まったが、大規模、複雑なシステムでは、そのアシュランスの議論も大規模化、複雑化する傾向があり、アシュランスケースを対象とするモジュール化が課題となっている[3,4]。

本論文では、アシュランスケースをモジュール化するための一般論構築へ向け、具体的事例を題材にモジュール化に取り組み、アシュランスケースをモジュール化する基準を模索する。

我々は帰属評価結果の妥当性を主張する形式アシュランスケースの構築を試み、報告した[5]。この形式アシュランスケースにはモジュール化がほとんどなされていない。本論文では、この形式アシュランスケースと同等な、しかしうまくモジュール化された形式アシュランスケースの構築を試み、次の観点からモジュール化を考察して、検討の結果を報告する。

- 題材およびその領域の必要事項を見極める、
- 題材の記述言語が提供するモジュールシステムを活用する。

最初の観点については、例えば次を考える必要がある。報告[5]の形式アシュランスケースには、測定、評価されたデータの品質、信頼性を主張する議論が記述されている。アシュランス議論はデータを引用

して進められる。この領域では、データを別のデータへ取り換え同じアシュランス議論をする可能性、データを再利用して別の品質、信頼性に関するアシュランス議論をする可能性がある。モジュール化はこのような発展可能性に柔軟に対応できることが求められる。

また、報告[5]で与えた形式アシュランスケースはAgda言語によって、データ型やデータ型の値の定義の集まりとして記述されている。Agda言語はモジュール化を支援する言語機構（module、importなど）を提供している。モジュールシステムを使い、形式アシュランスケースの中の型や値の定義をいかに、分類、分割して管理するかが課題である。

本論文の寄与は次の通りである：

- 題形式アシュランスケースのモジュール化の検討内容および基準を得た。また、形式アシュランスケースをモジュール化した具体例を得た。
- データの品質、信頼性を議論するアシュランスケースのモジュール化の具体例を与えた。
- アシュランスケースのモジュール化の一般論構築へ向けた具体的検討材料を与えた。

材料と方法

モジュール化と分解基準

ソフトウェアのモジュール化は。あらかじめ、運用時の保守、改修を容易にするため、将来の発展可能性を向上させるために行われる。

ソフトウェアエンジニアリングの教科書[2]には、モジュール化で期待される効果として次があげられている：

- 全体を単純な部品に分解できること。
- 逆に単純な部品を組合わせて全体を構成できること。
- 各部品は単純で簡単に理解できること。さらに、個々の部品を理解すれば、全体のシステムを理解できること。
- 変更、修正にも柔軟に対応できること。一部分を修正しても、それがいくつかの部分的な部品たちの修正に留まり、大がかりな全体の修正にまでつながらないこと。

実際にモジュールを設計するには分解基準が参考になる。プログラムに対しては、すでに、さまざまな分解基準が提案されている。例えば、Parnasは文献[1]で例題システムを用いて主要手順、情報隠蔽の二つの分解基準を説明および提案している。しかし、アシュランスケースに対しては、モジュール化のための分解機構[4]はあるが、具体的な基準はまだ検討の余地がある。

Agdaのモジュールシステム

Agda言語[6]が提供するモジュールについて必要な部分を簡単に紹介する。

モジュール宣言

Agdaのプログラムは型および関数などの定義からなる。Agdaではこれらをモジュールと呼ばれる部品に分割して管理する。例えば以下は、自然数を表す型の宣言NatとOneがNat型の値S Oである事の宣言の二つからなるモジュールM0の宣言である。

```
module M0 where
  data Nat : Set where
    O : Nat
    S : Nat → Nat
  One : Nat
  One = S O
```

モジュール内で定義された名前の参照

モジュールの中で定義された名前をモジュール名で修飾することによって、モジュールの外から参照することができる。例えば上記のモジュールM0の外からOneを参照するには

```
M0.One
```

とする。

パラメータ付きモジュール

モジュールには型や値のパラメータをつけることができる。例えば以下は型Tとその値tをパラメータとして受け取り、fがT型の値を全てtに写す関数である事の宣言を持つ付きモジュールM1の宣言である。

```
module M1 (T : Set) (t : T) where
  f : T → T
  f x = t
```

モジュールM1の外でM1.fを参照すると、これはTとtを仮引数とする関数を指す。従って例えば

```
M1.f (M0.Nat) (M0.O)
```

は型M0.Nat → M0.Natを持つ関数であり

```
M1.f (M0.Nat) (M0.O) (M0.S M0.O)
```

の値はM0.Oである。

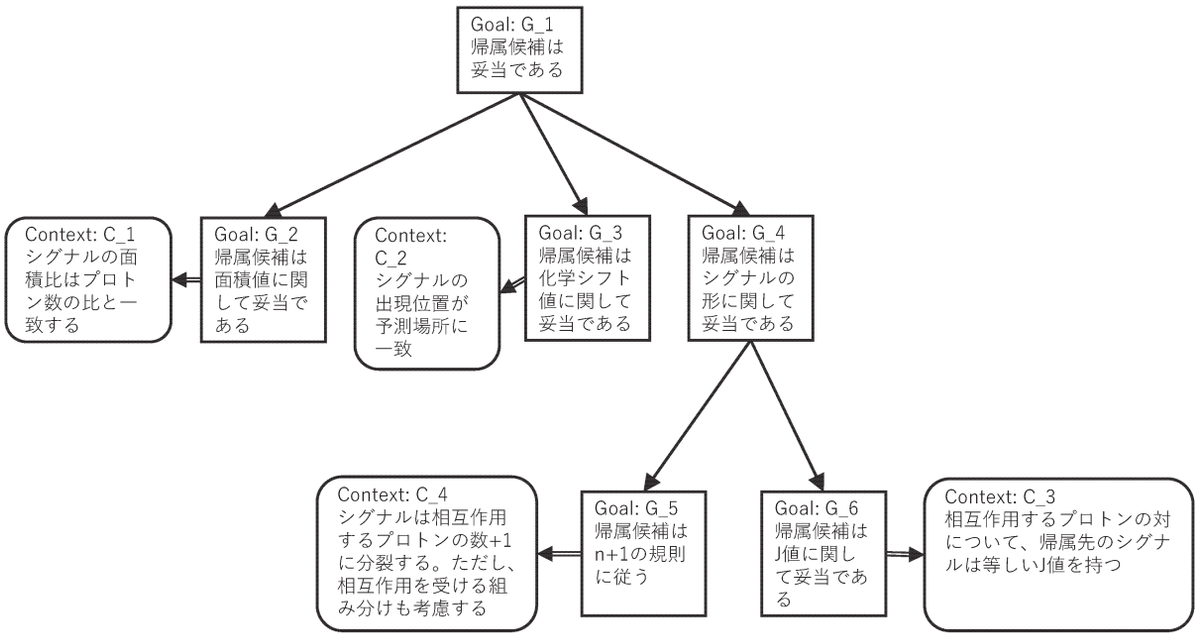

図 1. 題材の形式アシュランスケースの議論（概略）. 題材の形式アシュランスケースは，メタノールの 1H NMR スペクトルの帰属評価結果の妥当性を主張するアシュランスケースを形式化したものである. 測定サンプルの化合物の解析結果と測定データの解析結果の間の関係として与えられる帰属候補がそれぞれの解析結果に対して妥当であることを議論する. 詳細は報告 [5] を参照されたい.

モジュールを開く (open)

前節最後の式では Nat、S、O は全て M0 での定義を用いている。そこで、いちいち M0 で修飾するかわりに

```
open M0
```

としてモジュール M0 を「開く」と、その後では、M0 で定義された名前を M0 で修飾することなく

```
M1.f (Nat) (O) (S O)
```

などとして用いることができる。

形式アシュランスケース作成実験

データおよびプロセスの信頼性、品質を適切に伝えるための明文化する方法として、我々は形式アシュランスケースの適用可能性を検討している。

具体的には、産業技術総合研究所の有機化合物のスペクトルデータベース (SDBS) [7] が公開する「NMR スペクトルの帰属評価結果」を題材に、その妥当性を主張する議論をアシュランスケースおよび形式アシュランスケースで記述する実験を行ってきた [5,8]。

これまで、^{1}H NMR スペクトルの帰属評価結果数件を題材に、GSN（Goal Structuring Notation) の記法で記述したアシュランスケース事例を得た [8]。

さらに、そこで観察された課題を解決するため、得られたアシュランスケースの形式化を行った。その結果、これまで次の二種類の形式アシュランスケース事例を得ている。

1. スペクトルデータの解析結果の妥当性を主張する議論。
2. 帰属評価結果の妥当性を主張する議論。

両者のアシュランス議論は全く異なるが、引用するデータの部分など文脈に共通部分がある。このうち 2 について形式化のようすを報告した [5]。

本論文では、これまで報告してきた 2 の形式アシュランスケースを題材にモジュール化を検討する。ただし、モジュール化の検討を進める上で、2 と共通する文脈を持つ 1 の形式アシュランスケースのことも考慮する必要がある。以下では、1 のような 2 と文脈を共有するが異なる議論を記述したアシュランスケースのこと指して、2 に関連するアシュランスケースと呼ぶ。

帰属評価結果の妥当性を主張する形式アシュランスケース [5]

題材の形式アシュランスケースを紹介する。この形式アシュランスケースには図 1 の議論が記述されている。また、Agda のプログラムコードの全体構成は次のとおりである。(報告 [5] から引用)

1. 基本的な定義。
   コード全体にわたり使用する基礎的な型および関数を準備した。例えば、真偽値型、自然数型、浮

動小数点型からリスト型、ベクトル型とそれらに付随する関数など。

2. 文脈の定義
   アシュランスケースの文脈をまとめて表現した。
（ァ）解析結果データ、帰属候補
   メタノールについての議論で用いる測定データ、解析結果データを導入した。
（イ）専門家判断機構
   専門家判断の案件を格納するための準備。
（ウ）検査関数
   ゴールの要件が成り立つことを判断するため、データの検査関数を実装した。
3. ゴール
   アシュランスケースのゴールおよびサブゴールを準備した。
4. 証拠
   専門家判断の事実と事由を導入する。
5. ストラテジー
6. アシュランスケースの議論
   トップゴールの型の値を証明する。議論の木構造全体を表現する。

結果

検討内容

既存の形式アシュランスケースのプログラムコード、データの品質、信頼性の主張を明文化する領域の必要事項を解析した結果、以下の検討すべきモジュール化の要件を得た。

1. ゴールとストラテジー、ゴールと検査関数はそれぞれ結びつきが強く、分離しにくい。
（ァ）ゴールとストラテジーはコード上分離できない場合がある。レコード型を用いてゴールの型を定義する場合、ストラテジーはメンバーで表現される。
（ァ）ゴール（の構成子）と検査関数の定義を同時に修正しなければならない可能性がある。
2. データを導入する部分は二つに分かれる：個別のデータを格納するためのデータ型を定義する部分；データ型の値を実際に宣言してデータを導入する部分。
3. プログラム中の個々の定義は、個別の測定データに依存するものと全く依存しないものに分けられる。
4. データを取り換え、同じアシュランス議論をする必要がある。例えば、メタノールのスペクトルの帰属評価結果の妥当性の議論に換えて、エタノールのスペクトルの帰属評価結果について議論する。
5. 同じデータを使い、関連するアシュランス議論をする必要がある。例えば、メタノールの帰属評価結果でなく、同じメタノールのスペクトルデータの解析結果の妥当性を主張する議論をする。
6. 証拠の値はデータとゴールの両方に依存する。これは、値が、特定のデータがあるゴールを満足することを専門家が判断した事実に相当するため。

以上の要件を検討して次の基準を得た。

モジュール化の基準

我々がとったモジュール化の基準は、形式アシュランスケースを図 2 の五つのモジュールに分解するものである。

各モジュールの内容と役割りは次のとおりである。

共通語彙モジュール

帰属評価結果の妥当性を主張するアシュランスケースおよび、関連するアシュランスケースに共通する文脈はここにまとめる。

個別のデータを格納する型はここで定義する。

ゴールおよびストラテジーモジュール

帰属評価結果の妥当性を主張するアシュランスケースの議論で使うゴール、ストラテジー、検査関数を定義する。

個別データを格納するために導入する型および引用する個別データの値をパラメータに指定できるパラメータ付きモジュールとして実現する。

結果的に、ゴール、ストラテジーとゴールが成り

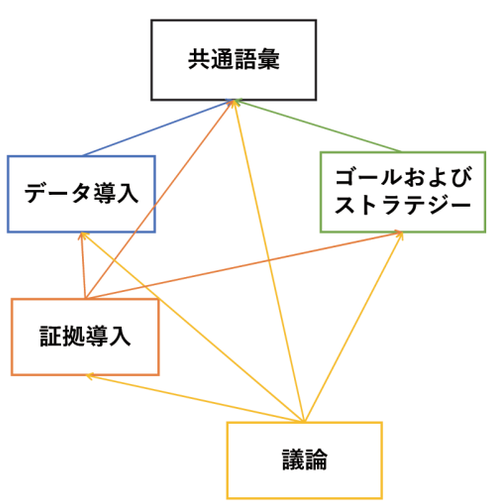

図 2. モジュール分解とモジュール間の依存関係．形式アシュランスケースを分解する五つのモジュールとモジュール間の依存関係を矢印で示したもの．例えば､議論モジュールから共通語彙モジュールへの矢印は，議論モジュールの中で共通語彙モジュールを開くことを意味する．

立つ要件がここへ集約される。

関連するアシュランスケースのゴールおよびストラテジーは帰属評価結果の妥当性のゴールおよびストラテジーとは別のモジュールにまとめる。

データ導入モジュール

共通語彙モジュールに定義された個別のデータを格納する型の値をここで定義して測定データ、解析結果データなどを導入する。

証拠導入モジュール

専門家判断結果型の値を定義して証拠を仮定として導入する。導入する証拠が無い場合はモジュールを置かなくても良い。

このモジュールは、データ導入モジュールとゴールおよびストラテジーモジュールを開いて定義を利用する。

ゴールおよびストラテジーモジュールを開くさい、実際のデータをパラメータに指定する。

議論モジュール

議論の木を構築する。
ここでは上記すべてのモジュール開き、定義を利用する。

基準の説明

我々は、データに依存する部分と依存しない部分を分けて区別した。ここでデータに依存しない部分とは、共通語彙モジュール、ゴールおよびストラテジーモジュールである。依存しないのはそれ以外のモジュールである。

データに依存する部分はひとまとめにせず、データ導入モジュール、証拠導入モジュール、議論モジュールの三つに分離した。分離した理由は、議論と独立にデータ導入モジュールを設けてデータを再利用できるようにするためである。

データに依存しない部分である、共通語彙モジュールとゴールおよびストラテジーモジュールも同様にひとまとめにしないことにした。これは関連するアシュランスケースがあることを考慮したためである。

モジュール化の具体例

以下に、前節で述べたモジュール化の基準に従ってモジュール分解した結果を紹介する。ここで、五つのモジュールはそれぞれ別々のファイルに分解した。

共通語彙モジュールは次の項目から構成される。項目 2 以降が測定データおよび解析結果などを格納するために準備する型定義である。

1. 基本的な型の準備
   1.1 量化記号、直和、maybe 型
   1.2 真偽値型
   1.3 自然数型
   1.4 記述説明データ型
   1.5 浮動小数点数型
   1.6 リスト型とベクトル型
   1.7 検査関数のひな形
2. ピークとシグナル
   2.1 ピーク
   2.2 シングレット
   2.3 マルチプレット
   2.4 シグナル
   2.5 シグナルの集まり
3. 測定化合物の解析結果型
4. 帰属候補型

ゴールおよびストラテジーモジュールは次の項目から構成される。最初に検査関数を定義して、次にそれらを利用してゴールおよびストラテジーを定義した。

1. 検査関数の定義
   1.1 専門家判断事実 - 型
   1.2 面積積分値の比較
   1.3 化学シフト値の比較
   1.4 結合定数の検査
2. ゴールおよびストラテジーの定義
   2.1 面積値について妥当
   2.2 化学シフト値について妥当
   2.3 N+1 の規則に従う
   2.4 結合定数について妥当
   2.5 シグナルの形状について妥当
   2.6 帰属候補は妥当

ゴールおよびストラテジーモジュールは次のプログラムコードのとおり、パラメータ付きモジュールとして宣言した。

```
open import 共通語彙
module ゴールおよびストラテジー (X : Set)
(DX : Peak-type X)
(signal-data : Signal-Data X DX)
(sample-data : Sample-Type)
(candidate
:Candidate-of-Assignment-Between
```

sample-data and signal-data) where

専門家判断事実の（構成子を持たない）型を共通語彙モジュールではなくこのモジュールの中で定義した理由は、専門家判断事実の値を導入できる場所をできるだけ制限するためである。ここで定義すれば、証拠の値はこのモジュールより上流に位置するモジュール、例えばデータ導入モジュールの中などでは定義できない。

データ導入モジュールは次の構成で与えた。

1. ピークデータ
2. シグナルデータ
3. 測定化合物の解析結果データ
4. 帰属候補データ

証拠導入モジュールおよび議論モジュールは単純なので構成を示すのは省略する。議論モジュールでは次のプログラムコードのように他の四つのモジュールを開いて、アシュランス議論を与える木を構成した。

```
open import 共通語彙
module 議論 where
  open import データ導入
  open import ゴールおよびストラテジー
 Peak-n  peak-d signal-d sample-d assign
  open import 証拠導入
```

ここで、特にゴールとストラテジーモジュールは具体的なパラメータを指定していることに注意されたい。パラメータとして指定しているのはデータ導入モジュールで定義した値たちである。

討論

形式アシュランスケースの既存研究の実例を題材にモジュール化に取り組んだ。得られた検討内容および基準を報告した。さらに、実際にモジュール化した事例を報告した。

モジュール化の基準で述べたように、データ導入モジュールおよび証拠導入モジュールが独立しているのが我々のモジュール化の特徴である。そのため、データと証拠の部分を取り換えること、データを取り換えず別アシュランス議論を構築するなど、モジュール化を進める前と比べアシュランケースが容易に再利用できるようになった。

本論文で報告したモジュール化の基準をもとに、一般的なアシュランスケースのモジュール分解基準へ発展させるのは今後の課題である。

謝辞

本研究は、研究課題「システムライフサイクルとそのアシュランス議論の Agda による定式化」に対する 2017 年度神奈川大学総合理学研究所の共同研究助成（RIIS201703）を受けた。

文献

1) Parnas DL (1972) On the criteria to be used in decomposing systems into modules. *Commun. ACM* 15. **12**: 1053-1058. [DOI=http://dx.doi.org/10.1145/361598.361623].
2) Ghezzi C, Jazayeri M and Mandrioli D (2002) *Fundamentals of Software Engineering (2nd ed.)*. Prentice Hall PTR, Upper Saddle River, NJ, USA.
3) Kinoshita Y and Takeyama M (2013) Assurance case as a proof in a theory: towards formulation of rebuttals. In : *Assuring the Safety of systems – Proceedings of the Twenty-first Safety-critical Systems Symposium*, *Bristol, UK*. Dale C and Anderson T, eds., CreateSpace Independent Publishing Platform, Bristol. pp. 205-230.
4) The Assurance Case Working Group (ACWG) (2018) *Goal Structuring Notation Community Standard. Version 2*. SCSC - The Safety-Critical System Club, UK. [https://scsc.uk/r141B:1].
5) 渡邊　宏 , 木下佳樹 , 武山　誠 , 奥野康二 (2017) 形式アシュランスケース事例：メタノール ^{1}H NMR 帰属評価結果の妥当性 — SDBS の帰属および帰属決定プロセスについてのアシュランスケースの研究 —. *Sci. J. Kanagawa Univ.* **28**: 37-45.
6) The Agda Team, Agda Documentation. [http://agda.readthedocs.org/].
7) 国立研究開発法人 産業技術総合研究所 有機化合物のスペクトルデータベース (SDBS). [https://sdbs.db.aist.go.jp].
8) 渡邊　宏 , 木下佳樹 , 武山　誠 , 奥野康二 (2016) SDBS の帰属および帰属決定プロセスについてのアシュランスケースの研究 . *Sci. J. Kanagawa Univ.* **27**: 29-38. [http://hdl.handle.net/10487/14213].